identifying information (but rather as call content), this treatment plainly does not render the standard deficient.

The implication of the DOJ/FBI Petition that post-cut-through dialing information is not available to law enforcement under J-STD-025 is entirely misleading. The standard emphatically does permit law enforcement to obtain access to all post-cut-through digits – in either of two ways.[100] **First**, the information is available on the content channel provided by the carrier conducting the initial intercept, because post-through-digits are transmitted on the content channel just like any other content. This information is available to law enforcement pursuant to a Title III content intercept order. In fact, in December 1997, the FBI agreed that carriers can make post-cut-through digits available to law enforcement by "provid[ing] CCC [the call content channel] to law enforcement for deciphering[.]"[101]

Second, post-cut-through dialing information is available pursuant to a pen register order or subpoena directed to the long-distance carrier that actually completes the second call. Because the digits are dialed before cut-through by the second carrier (i.e., they are not post-cut-through information with respect to the second carrier), they are available as call-identifying information. There is absolutely no requirement under CALEA that local exchange carriers bear the burden of obtaining such information that is in the

---

[100] See CDT Petition at 13 ("Law enforcement wishing to intercept these post-cut-through digits has two choices: serve the first carrier with a content interception order, or serve the long-distance carrier, which does treat the digits as call-identifying information, with a pen register order.").

[101] FBI December 1997 Clarifications at 2.

possession of other parties. The legislative history of CALEA makes this point in a slightly different context:

> If, for example, a forwarded call reaches the system of the subscriber's carrier, that carrier is responsible for isolating the communication for interception purposes. However, if an advanced intelligent network directs the communication to a different carrier, the subscriber's carrier only has the responsibility . . . to ensure that law enforcement can identify the new service provider handling the communication.[102]

That is, the obligation to seek information in the possession of third parties lies with law enforcement. The fact that this obligation may not satisfy the desire of law enforcement for maximum convenience is no basis for creating CALEA obligations that Congress did not intend.

The real agenda of DOJ and FBI with respect to post-cut-through dialing information is to be able to obtain the information through a pen register order issued only to the carrier conducting the initial intercept, in order to avoid inconvenience and other requirements associated with the two approaches described above.[103] While TIA is sympathetic with law enforcement's desire to make its job as easy as possible, this is not a proper basis for assertion of CALEA obligations. Moreover, there are at least three independent reasons that CALEA does not require that post-cut-through digits be provided as call-identifying information pursuant to a pen register order.

---

[102] CALEA House Report at 22.

[103] See, e.g., id. at 40 n.18. A pen register order is available under a lower legal standard than a Title III interception order. Title III orders also have additional requirements such as live monitoring and minimization that provide additional burdens and costs on law enforcement. Thus, law enforcement has the incentive to try to avoid such burdens and costs if they can get away with it.

First, post-cut-through digits are not call-identifying information for the initial carrier. The initial carrier generally does not need to use the digits for call routing (or any other purpose), and therefore does not detect the digits in its switch. The CDT Petition makes this point: "To the system of the local exchange carrier complying with a surveillance order, the call has been properly routed and any further dialed digits are treated as indistinguishable from other content."[104] That is, for a local exchange carrier, it is irrelevant whether post-cut-through communications consist of dialed digits, a fax transmission, or a whispered conversation between two lovers. Post-cut-through digits are only call-identifying information for the second carrier that uses the digits for call routing, and it is only from the second carrier that the information may be properly sought under a pen register order.

Second, post-cut-through digits are not "reasonably available" to the first carrier as call-identifying information. As a technical matter, modern switches detect dialed digits with a "tone receiver," which is only connected to a call circuit until the call is completed (i.e., cut through). At that point, the tone receiver is available for use on another call. Because tone receivers can be repeatedly used in this manner, manufacturers build switches with a number of tone receivers that is far lower than the number of simultaneous calls that the switch can support. Therefore, it would require major system modifications to dedicate a tone receiver for the duration of each call, which would be necessary to detect post-cut-through digits and deliver them to law enforcement.

[104] CDT Petition at 13.

Costly switch modifications without any business justification would be needed to provide such capability.

Moreover, new technologies, such as voice-recognition dialing, would require even more complicated technologies to detect post-cut-through digits. Voice-recognition dialing permits a subscriber to call a second telecommunications carrier and then to speak or "voice dial" the name of a person or destination, whose number is dialed by the second carrier. In order for the subscriber's original carrier to provide post-cut-through digits for such calls, it would need to directly integrate its network intercept facilities with the equipment or databases of the second carrier, or possibly to install voice-recognition hardware and software in its own switches. Carriers have no way to implement such technical solutions, nor do they have any business reason to do so. Furthermore, CALEA specifically provides that law enforcement cannot mandate particular designs of "equipment, facilities, services, or system configurations."[105]

In sum, there should be no question that post-cut-through digits are not reasonably available as call-identifying information.

Third, the delivery of post-cut-through dialing information pursuant to a pen register order would not protect "the privacy and security of . . . call-identifying information not authorized to be intercepted . . . ."[106] As noted above, post-cut-through digits include credit card numbers and other substantive information such as responses to an automatic queuing system. Such substantive information may not be disclosed pursuant to a pen

---

[105] 47 U.S.C. § 1002(b)(1).

[106] 47 U.S.C. § 1002(a)(4)(A).

register order. Indeed, CALEA specifically amended the pen register provisions of Title III to place limitations on the authority of law enforcement to obtain such information pursuant to a pen register order:

> LIMITATION – A government agency authorized to install and use a pen register . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.[107]

Furthermore, in analogous circumstances, the Fourth Circuit concluded in Brown v. Waddell[108] that disclosure pursuant to a pen register order is impermissible. Brown involved the question whether a police officer could obtain numeric messages being sent to the target's display pagers, under the authority of a pen register order. The court held that the pen register authorization was not sufficient, because the pager could receive "substantive information."[109]

A telecommunications carrier would have no means of segregating protected information which is not subject to a pen register order from digits used for call routing. Because not all post-cut-through digits could legally be disclosed, and because the carrier would not be able to distinguish among post-cut-through digits, carriers cannot be required to deliver post-cut-through information pursuant to a pen register order. Therefore, J-STD-025 appropriately does not treat such information as call-identifying information.

---

[107] 18 U.S.C. § 3121(c), added by Section 207(b) of CALEA.

[108] 50 F.3d 285 (4th Cir. 1995).

[109] Id. at 292.

2. Subject-Initiated Signaling

Subject-initiated signaling activity, as addressed in the DOJ/FBI Petition, takes place when an intercept subject has subscribed to services such as call forwarding and call transfer, and uses "feature keys" (such as a transfer key) or uses the "flash hook" (this usually means briefly depressing the hook used to hang up the telephone, but on some telephones it involves the use of a separate "flash" key).[110]

Subject-initiated signaling activity is not call-identifying information, because it does not "identif[y] the origin, direction, destination, or termination of [a] communication."[111] DOJ and FBI argue that the information is call-identifying information, because it is needed "to identify the destination of each communication," and to preserve law enforcement's ability to intercept communications involving features such as call forwarding, speed dialing and conference calling.[112] They contend that if this information is not available, "law enforcement will be left with an incomplete and potentially inaccurate evidentiary picture of the subject's . . . signaling activities incidental to his calls."[113]

But DOJ and FBI offer no evidence that failure to provide information on all subject-initiated signaling activity will impair the ability of law enforcement to determine the destination of communications. The DOJ/FBI Petition does not identify any specific subject-initiated signaling activity that is both required by CALEA and is not already

---

[110] See DOJ/FBI Petition at 36.

[111] 47 U.S.C. § 1001(2); see also CDT Petition at 14 (flash hooks and feature keys "do not fit within the definition of 'call-identifying' information in CALEA").

[112] DOJ/FBI Petition at 38.

[113] Id. at 37.

required to be provided under J-STD-025. The absence of such specifics means that there is likewise an absence of any basis on which the Commission could find J-STD-025 to be deficient in this area.

In fact, J-STD-025 requires provision of all reasonably available call-identifying information that DOJ and FBI could obtain from subject-initiated signaling activity. This information falls into two categories: (1) signaling activity that is transmitted from the subscriber to the network (and detected by the switch) and (2) signaling activity that controls local functions of the subscriber's equipment.

First, with respect to network-detected signaling activity, J-STD-025 requires provision of all potentially-relevant call-identifying information. Specifically, the "Change" message specified in J-STD-025 is provided when:

- two or more call identities are merged into one call identity;
- an additional call identity is associated with an existing call;
- a call identity is split into two or more call identities; or
- a call identity is changed to another call identity.[114]

The "Redirection" message is provided when:

- an incoming call attempt to the intercept subject is forwarded (e.g., call forwarding or call diversion);
- an incoming call attempt to the intercept subject is deflected (e.g., call waiting deluxe or call deflection); or
- an incoming call attempt to an intercept subject with terminal or personal mobility is redirected to the intercept subject's current location (e.g., call delivery).[115]

[114] J-STD-025 § 5.4.4.

J-STD-025 also requires provision of information on the destination of any outgoing call (including calls made by speed dialing),[116] the origin of any incoming call,[117] and the termination of any active call.[118]

This information required by J-STD-025 is fully sufficient to give law enforcement all relevant call-identifying information provided by subject-initiated, network-detected signaling activity (including for the services identified in the DOJ/FBI Petition – call forwarding, speed dialing and conference calling).[119] The only additional information that would be available under the DOJ/FBI request is the identity of the actual keys pressed by the intercept subject. It should be readily apparent that this information is not required by CALEA, where J-STD-025 already requires provision of all relevant information on the effect in the network of the use of the keys. For example, if law enforcement knows that an intercept subject transfers to another call through use of call waiting, it is not necessary to know whether the subject pressed the hang-up key or a specialized "flash" key.

---

[115] Id. § 5.4.7.

[116] See id. § 5.4.5 (Origination message), Annex D.14 (example of use of Origination message for speed calling).

[117] See id. § 5.4.10 (TerminationAttempt message), § 5.4.1 (Answer message).

[118] See id. § 5.4.8 (Release message).

[119] J-STD-025 does not require provision of information to law enforcement when a party is placed on hold. See, e.g., id. Annex D.9 (describing data message for a call held and retrieved). However, this information is of no relevance in a two-party call, since the call content channel indicates whether a conversation is proceeding between the parties. The use of the hold key in connection with a multi-party call is discussed in section III.B below.

Second, certain calls involve local signaling activity (e.g., signaling that is internal to a private branch exchange ("PBX")) that is not detected by a telecommunication carrier's network. However, even for such calls, J-STD-025 provides that the carrier will supply to law enforcement the destination of outgoing calls, the origin of incoming calls, and the termination of any such call.[120] As pointed out above, any additional information provided by local signaling activity is not call-identifying information because it does not "identif[y] the origin, direction, destination, or termination of [a] communication."

More importantly, even if the Commission were to conclude that some local signaling activity constitutes call-identifying information, local signaling activity is for obvious reasons not "reasonably available" to the carrier. Such information is not used at all by the carrier, and there is no reason to build networks to detect it. Furthermore, the legislative history of CALEA explicitly indicates that the statute is inapplicable to customer equipment like PBXs:

> The bill does not cover private branch exchanges (PBX's). This means that there will be times when the telecommunications carrier will be unable to isolate the communications of a specific individual whose communications are coming through a PBX.[121]

---

[120] In the context of PBXs, provision of such information may require intercept orders covering trunk communications, which may not always be granted by a court. The legislative history of CALEA states that "[t]he Committee does not intend the exclusion of PBX's to be read as approval for trunk line intercepts." CALEA House Report at 24. Although CALEA does not cover PBXs, an intercept order can be directed to the custodian of the PBX under Title III authority that was not changed by CALEA. See generally 18 U.S.C. §§ 2516-2518.

[121] Id.

In order for carriers to make local signaling information available to law enforcement, equipment manufacturers would need to design (and carriers would need to purchase) new signaling systems between subscriber equipment and switches. Such modifications would serve no business purpose, would be extremely expensive, and would certainly have a significant impact on ratepayers. Accordingly, a requirement to provide such information would be inconsistent with at least three provisions of CALEA: (1) the limitation that only "reasonably available" call information must be delivered to law enforcement,[122] (2) the limitation that law enforcement may not require specific design of carrier networks,[123] and (3) the requirement that the Commission prescribe only "cost-effective methods" and "minimize the cost . . . on residential ratepayers" in acting on a deficiency petition like the DOJ/FBI Petition.[124]

B. Party Hold / Party Join / Party Drop

The DOJ/FBI Petition also requests delivery of certain "information on participants in a multi-party call,"[125] which was referred to in the punch list as "party hold, party join, party drop."[126] This capability would require a carrier to generate a data message for law enforcement when a party to a multi-party call is placed on hold by the

---

[122] 47 U.S.C. § 1002(a)(2).

[123] See 47 U.S.C. § 1002(b)(1).

[124] 47 U.S.C. § 1006(b)(1), (3).

[125] See DOJ/FBI Petition at 42-45.

[126] See Colgate Letter at 2 & Attachment A.

intercept subject, a party (including a party on hold) joins a multi-party call, or a party is dropped from a multi-party call.[127] The requested capabilities are limited to parties to conference calls that are supported by the services of the intercept subject.[128]

This requested capability presents much less significant issues than are apparent from the DOJ/FBI Petition, because J-STD-025 already requires provision of information that substantially satisfies the "party join" and "party drop" capabilities requested by DOJ and FBI. With respect to "party join," the J-STD-025 Origination, TerminationAttempt and Change messages require provision of a data message to law enforcement when a party joins a multi-party call supported by the subscriber's facilities – either through initiation by the subscriber of a call to a new party who is added to the call,[129] or through receipt of a call from a new party who is added to the call.[130] With respect to "party drop," the J-STD-025 Release message requires provision of a data

---

[127] See DOJ/FBI Petition at 43.

[128] See DOJ/FBI Petition at 42 ("A subscriber may subscribe to services or features that would support a multi-party call. If so, various associates can be added to, placed on hold during, or dropped from the call."). It is plain that CALEA would not require provision of call-identifying information on multi-party calls supported by facilities or services of a person other than the intercept subject (e.g., where the intercept subject participates in a conference call arranged by a conference call service), except to the extent of the intercept subject's participation in such a call. That is, J-STD-025 requires provision of all call content and reasonably available call-identifying information regarding the participation of the intercept subject in such a call, including the content of the conversations of all parties who can be heard by the intercept subject.

[129] See J-STD-025 § 5.4.5 (Origination message), § 5.4.4 (Change message), Annex D.10 (examples of messages generated for three-way calling).

[130] See J-STD-025 § 5.4.10 (TerminationAttempt message), § 5.4.4 (Change message), Annex D.10 (examples of messages generated for three-way calling).

message when a party is released from a multi-party call.[131] To the extent that DOJ and FBI believe that there is reasonably available information on "party join" and "party drop" that is not provided by J-STD-025, the burden should be on DOJ and FBI to identify such information with specificity. The Commission should not require TIA to include new data messages in J-STD-025, based upon unsupported blanket allegations by DOJ and FBI regarding the "deficiencies" of J-STD-025. TIA believes that, in fact, no such deficiencies exist. TIA hereby requests a further opportunity to respond to any claims by DOJ and FBI that they have identified particular deficiencies.

Thus, the primary disputed issue regarding party hold/party join/party drop capabilities is the fact that J-STD-025 does not require any message when a participant is placed on hold (or released from hold) by the intercept subject.[132] The absence of such a "party hold" provision in J-STD-025, however, does not provide a basis for concluding that the standard is "deficient," for several reasons.

First, and most important, "party hold" information is plainly not call-identifying information.[133] It is clear that the fact that a party is or is not on hold does not

---

[131] See J-STD-025 § 5.4.8 (Release message), Annex D.10 (examples of messages generated for three-way calling).

[132] J-STD-025 also does not require provision of "party join" and "party drop" information when these functions are performed by customer equipment, such as a PBX or a multi-line telephone. However, under such circumstances "party join" and "party drop" information is not "reasonably available" for the same reasons set out in section II.A.2 above regarding local (i.e., non-network-detected) signaling information.

[133] See CDT Petition at 14 (party hold/party join/party drop "messages do not relate to call-identifying information but rather seek to enhance law enforcement investigative techniques beyond the status quo").

"identif[y] the origin, direction, destination, or termination of [a] communication." This consideration alone should conclusively determine that CALEA does not require provision of "party hold" information.

Second, to the extent a party is placed on hold by a hold key that is a feature local to the subscriber's equipment – and thus is not detected by the network – "party hold" information is not "reasonably available" to a telecommunications carrier, for the same reasons set out in the discussion of local signaling information in section II.A.2 above.

Third, the DOJ/FBI rationale for requesting party join/party hold/party drop information is that "[w]ithout these messages, law enforcement would not know who joins or leaves a conference call, whether the subject alternated between calls, or which parties heard or said parts of a conversation."[134] This rationale is unpersuasive with respect to "party hold" information. Although the absence of "party hold" information could prevent law enforcement from being certain that a party heard particular conversations during a multi-party call, the same uncertainty would also be present if party hold information were available – for the simple reason that a party can walk away from the phone or stop listening even without being placed on hold. Ultimately, the only persuasive evidence that a party heard an intercepted statement is the fact that the party responded to the statement.

Fourth, DOJ and FBI explicitly acknowledge that party hold information has not historically been available on wiretaps.[135] Thus, even under their sweeping "always

---

[134] DOJ/FBI Petition at 43.

[135] See DOJ/FBI Petition at 44.

been available" reading of the statute, CALEA does not require carriers or manufacturers to supply this information.

C. Network-Generated In-Band and Out-of-Band Signaling

The DOJ/FBI Petition requests delivery of "in-band" and "out-of-band" signaling information that is generated by the network.[136] While the Petition itself provides only limited specificity regarding the nature of such information, the Proposed Rule[137] offered by DOJ and FBI defines the information to include:

> (A) any alerting of incoming calls or messages;
>
> (B) audible indications of incoming calls or messages (e.g., call waiting tone, message waiting tone, power alert/ring, distinctive alert/ring, recall alert/dial tone, call forwarding reminder alert/ring, busy tone, or reorder tone);
>
> (C) visual indications of incoming calls or messages (e.g., lights to indicate call waiting); and
>
> (D) alphanumeric display information (e.g., messages sent to the terminal, calling number identification, or calling name identification).[138]

This request for a wide variety of disparate types of network signaling information is emblematic of the approach that DOJ and FBI have taken throughout the standards process: requesting as much as possible without conducting a serious analysis of whether each particular element of the request is supported by CALEA. As recently as

---

[136] See DOJ/FBI Petition at 45-47.

[137] See id. at Appendix 1, Proposed Final Rule ("Proposed Rule").

[138] Proposed Rule § 64.1708(d)(1).

December 1997, the FBI stated that it is "[n]ot interested in all network signals [but is] interested in defined sub-set of user perceived signals."[139] Despite this recent concession, the DOJ/FBI Petition contains no reasoned limitations on the requested capabilities, which should weigh heavily against a Commission conclusion that J-STD-025 is "deficient" with respect to provision of network-generated signaling information. In any event, in the case of the information listed in the Proposed Rule, each of the items requested is either already provided under J-STD-025, or is not call-identifying information required to be provided by CALEA.

First, with respect to "alerting of incoming calls or messages," the TerminationAttempt message defined in J-STD-025 requires provision of a message at the time of each incoming call.[140] The meaning of "incoming message" in the Proposed Rule is unclear, since the term "message" is undefined in the Proposed Rule and J-STD-025 does not cover paging. To the extent this refers to an alert to the subscriber that a message is waiting, it is addressed below.

Second, with respect to audible signaling information, J-STD-025 requires provision of data messages that convey all of the relevant call-identifying information that is conveyed by audible signaling. For example, the following capabilities are requested in the DOJ/FBI Petition and the Proposed Rule:

- a busy signal indicates only the reason that a call was not answered (which is not call-identifying information), while J-STD-025 requires

---

[139] FBI December 1998 Clarifications at 2.

[140] See J-STD-025 § 5.4.10.

provision of the relevant call-identifying information – i.e., the number dialed and whether the call was answered;[141]

- a call-waiting signal provides information that is required to be provided by J-STD-025 – i.e., the fact of an incoming call;[142]
- a call-forwarding reminder alert/ring provides information that is required to be provided by J-STD-025 – i.e., the fact that a call was re-directed;[143] and
- a "stutter" dial tone indicates only that a voice mail message is waiting (which is not call-identifying information), while J-STD-025 requires provision of the relevant call-identifying information – i.e., the fact of an incoming call that was not answered.[144]

While this list does not exhaustively cover all types of audible signaling, the burden should be on DOJ and FBI to identify the specific respects in which J-STD-025 fails to provide relevant call-identifying information – something the DOJ/FBI Petition simply fails to do. TIA is confident that, in fact, it will not be possible for DOJ and FBI to identify any such deficiencies. TIA hereby requests a further opportunity to respond to any claims by DOJ and FBI that they have identified particular deficiencies.

Furthermore, J-STD-025 requires that most audible signaling information be provided over the call content channel. For subject-originated calls, the standard contemplates that the call content channel will be available to law enforcement as soon as the subject is "off-hook."[145] For calls received by the subject, the standard provides that

---

[141] See id. § 5.4.1 (Answer message), § 5.4.5 (Origination message).

[142] See id. § 5.4.10 (TerminationAttempt message).

[143] See id. § 5.4.7 (Redirection message).

[144] See id. § 5.4.1 (Answer message), § 5.4.10 (TerminationAttempt message).

[145] See id. Annex D.

"[l]oss of any portion (i.e., the beginning, middle, or end) of call content should not occur between call completion (answer) and call release."[146]

The DOJ/FBI Petition recognizes that "[t]his information historically has been available to law enforcement on call content channels"[147] – that is, it has been provided in just the manner that J-STD-025 requires. Even more important, the FBI recently conceded that it is willing to accept access to audible signaling information on the call content channel, although it would "prefer" separate data messages regarding the signaling.[148] Clearly, a law enforcement "preference" is no basis for imposition of a CALEA "obligation."

Although the above bases are fully sufficient for denying the DOJ/FBI request for audible signaling information, it is also important to note that a significant proportion of audible signaling information is not reasonably available to carriers. Specifically, where audible signaling information is produced by a remote network, the local switch does not have any reason to detect the signaling information. For example, in the frequent circumstance where a subscriber makes a long-distance call, the ring or busy signal for the called party is generated by the switch of a carrier other than the subscriber's carrier.[149]

---

[146] Id. § 4.5.1.

[147] DOJ/FBI Petition at 46.

[148] FBI December 1997 Clarifications at 2 ("Some user-perceived signals can be heard on the CCC and in those circumstances LE is willing to accept access to the CCC as opposed to separate signals on the CDC, but would prefer a separate message on the CDC[.]").

[149] The subscriber's switch senses only whether the subscriber continues the call (which would likely happen if it is answered) or hangs up (which would likely happen if there is a busy signal or no answer). In any event, it is the subscriber's action and not the remote audible signaling information that is detected by the local switch.

Switches do not sense audible tones generated by remote networks, and would require installation of new equipment to be able to so. Such equipment would serve no network purpose, and would increase the cost of telecommunications equipment (and ultimately the cost of service).

In addition, the DOJ/FBI Petition states that "digital switching and new technology have given rise to network-generated call progress messages that are not available over call content channels."[150] However, the petition does not identify any specific type of such digital signaling information that is required to be provided by CALEA, and that is not provided by J-STD-025. Furthermore, the DOJ/FBI Petition does not explain why the assistance provided under J-STD-025 would be less effective in a fully digital network. To the contrary, the requirements of the J-STD-025 are technology-independent[151]; that is, the standard requires the provision of the same call-identifying information whether a network uses audible or digital signaling. As explained above, J-STD-025 requires provision of all reasonably available call-identifying information for network events identified by DOJ and FBI that involve audible signaling, and the same information would be available for the same network events where digital signaling is used.

Third, with respect to visual signaling information, the DOJ/FBI Petition asserts the specific signals generated by an unanswered phone (e.g., rings or a flashing light) are call-identifying information, because, "[f]or example, criminals may use ringing

---

[150] DOJ/FBI Petition at 46.

[151] See J-STD-025 § 4.4 ("A call event is a user action or signal that may cause a call state to change. These events are not intended to reflect a particular technology, but to describe the event in general.").

signals as a way of conveying pre-arranged messages to each other without having to engage in direct conversations over the phone system."[152] This argument stretches the government's "parade of hypotheticals" mode of analysis past the breaking point, and the Commission should summarily reject it. There is no serious argument that such ring signaling is call-identifying information that "identifies the origin, direction, destination, or termination of [a] communication." One criminal might also signal another by throwing a cell phone at him, but the mere fact that a telephone is involved does not mean that CALEA requires provision of detailed information on this "telephone toss" signal. For incoming unanswered calls, J-STD-025 requires provision of information on the fact of the incoming call, the number at which it originated, and the fact that it was not answered[153] – CALEA certainly requires no more.

Fourth, with respect to "alphanumeric display information," the TerminationAttempt message specified by J-STD-025 requires provision of the telephone number of the calling party, even if the intercept subject does not subscribe to "Caller ID" service and therefore does not receive such a message.[154] The DOJ/FBI Petition and the Proposed Rule do not identify any other "alphanumeric display information" that constitutes call-identifying information: "calling name information" provides no call-identifying

---

[152] DOJ/FBI Petition at 45.

[153] See J-STD-025 § 5.4.10 (TerminationAttempt message); § 5.4.1 (Answer message).

[154] See id. § 5.4.10 (TerminationAttempt message).

information that is additional to "calling number information";[155] and the Proposed Rule does not explain what types of "messages sent to the terminal" would constitute call-identifying information.[156]

In sum, there is no basis for the Commission to find J-STD-025 deficient with respect to the provision of network-generated signaling information.

D. Delivery of Call-Identifying Information on Call Data Channel

The DOJ/FBI Petition also requests that all call-identifying information be delivered on the call data channel ("CDC"), even where the information is already available on the call content channel under J-STD-025. However, DOJ and FBI explicitly "agree that a carrier could comply with its delivery obligations under Section 103 without delivering this information in this fashion."[157] DOJ and FBI deserve praise for their candor; for this concession demonstrates clearly that they have no claim that J-STD-025 is deficient in this area.

After recognizing that the requested capability is not required by CALEA, the DOJ/FBI Petition urges nonetheless that telecommunications carriers deliver call-identifying information on the CDC because this is the "most efficient and effective means

---

[155] In fact, "calling name information" provided by a network database is likely to be incorrect if the calling party is not using his or her own telephone.

[156] It is important to note that J-STD-025 covers circuit-switched and packet-switched telephony, and not paging. Therefore, there is no basis for the Commission to find J-STD-025 deficient for failure to cover paging-like alphanumeric messages.

[157] DOJ/FBI Petition at 47; see also FBI December 1997 Clarifications at 2 ("[s]ome user-perceived signals can be heard on the CCC and in those circumstances LE is willing to accept access to the CCC").

of delivering authorized surveillance information to law enforcement."[158] And where, one might ask, is this standard to be found in CALEA? The answer is – nowhere. The only provisions of CALEA that DOJ and FBI cite in support of this notion are provisions relating to law enforcement-industry consultations and government payment of costs for CALEA compliance.[159] The Commission should recognize that this argument is entirely lacking in legal force.

Indeed, there is a broader lesson in this claim. DOJ and FBI have advanced it without regard for the statutory language and without regard even for the interpretation of CALEA advanced earlier in their own brief – that CALEA gives law enforcement those wiretap features that it previously received in the days of alligator clips. Law enforcement has never received all of its information on the call data channel.

Finally, this capability has been added at the last possible moment; it was not included on the original punch list,[160] and it was not formally raised by law enforcement until the DOJ/FBI Petition was filed. Indeed, if the Commission wishes to understand some of the reasons for extensive delays in the standards process and for frayed FBI-industry relations, it need look no further than this "last-minute" request, which DOJ and

---

[158] DOJ/FBI Petition at 47. It may be that another purpose of DOJ and FBI is to have the opportunity to seek to obtain all call-identifying information pursuant to a pen register order. However, this purpose is not articulated in the DOJ/FBI Petition, likely because CALEA makes clear that a request for such information pursuant to a pen register order would be improper. See Section 207(b) of CALEA, 18 U.S.C. § 3121(c) (limiting information available on a pen register order to "dialing and signaling information utilized in call processing").

[159] See DOJ/FBI Petition at 48 (citing 47 U.S.C. §§ 1006(a)(1), 1008).

[160] See Colgate Letter at Attachment A.

FBI recognize to lack legal authority and which has been raised in this proceeding for the first time. This is unfortunately all too typical of the conduct of the FBI over more than three years of negotiations with industry over CALEA implementation. The DOJ/FBI agenda has been to demand an ever-growing list of expansive, burdensome wiretap obligations from industry, without regard for a consistent – or even plausible – interpretation of CALEA.

E. Timing of Call-Identifying Information

The DOJ/FBI Petition seeks delivery of call-identifying information within three seconds of the event producing the call-identifying information, together with a time stamp indicating the timing of the event to an accuracy of 100 milliseconds (one tenth of a second).[161] These specific timing requirements are inconsistent with the capabilities of existing telecommunications networks. They also lack any basis in CALEA, as DOJ and FBI are once again candid enough to admit, noting that "[t]he particular timing requirements in the proposed rule are not the only ones that would satisfy Section 103(a)(2)."[162]

The DOJ/FBI Petition relies on colorful examples – a "contract murder," a ransom call, and a bomb threat[163] – to support the argument that a few seconds or milliseconds of extra time are needed to preserve the efficacy of law enforcement in such

---

[161] See DOJ/FBI Petition at 49-52.

[162] Id. at 52.

[163] See id. Petition at 49, 52.

emergency situations. While such scenarios are easy to conjure up, the DOJ/FBI Petition cites only imaginary cases. Despite access to thirty years' worth of actual wiretaps and prosecutions, DOJ and FBI cite not a single actual case where split-second delivery of data was crucial. Perhaps, the DOJ/FBI Petition does not cite history because history is not helpful to its argument. The reality is that the timely delivery requirements of J-STD-025 give response time to law enforcement at least comparable to what it has historically received in intercept cases. In addition, CALEA and J-STD-025 require delivery of intercept information to a location (usually a law enforcement headquarters office) specified by law enforcement,[164] a requirement which provides much greater response flexibility to law enforcement than that available in local loop interceptions. Thus, the implication of the DOJ/FBI Petition that failure to adopt the requested timing obligations raises safety concerns is unwarranted.

Equally unwarranted is the DOJ/FBI claim that these timing requirements are required by CALEA. The DOJ/FBI request actually involves two separate capabilities: expeditious delivery (i.e., within three seconds of the triggering event) and synchronization of the CDC with the triggering event (i.e., within 100 milliseconds). It is hard to say which of these demands is farthest from Congressional intent – the first, which is expressly rejected by the language of CALEA, or the second, which has no basis in the statute whatsoever.

[164] See 47 U.S.C. § 1002(a)(3); J-STD-025 § 4.2.2.

1. Expeditious Delivery

DOJ and FBI demand that information about events during a call be provided within three seconds of each event. This demand is rebutted by the text of the statute. CALEA requires telecommunications carriers to "expeditiously" provide law enforcement access to reasonably available call-identifying information "before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government)."[165] Since Congress certainly envisioned telephone calls lasting longer than three seconds, allowing delivery of call identifying information after the call is flatly inconsistent with the DOJ/FBI position.

J-STD-025 implements the statutory requirement of expeditious delivery[166]; indeed, it contemplates that call-identifying information will be provided to law enforcement as soon as it is generated, except where the CDC becomes congested.[167] That is, J-STD-025 requires delivery of call-identifying information "before, during, or immediately after" a communication, except where law enforcement has not ordered the provisioning of a sufficient number of CDCs to support ongoing interceptions without congestion. Since the number of CDCs used in wiretaps is within the control of law enforcement, not telecommunications carriers, delays caused by insufficient CDCs are by definition "acceptable to the government."

---

[165] 47 U.S.C. § 1002(a)(2) (emphasis added).

[166] See J-STD-025 § 4.4 ("The Call-Identifying Information IAP (IDIAP) . . . provides expeditious access to the reasonably available call-identifying information for calls made by an intercept subject or calls made to an intercept subject.") (emphasis added).

[167] See id. § 4.6.2 ("When the call-identifying information intercept communication resources (e.g., CDCs) are limited, the communications are accessed on a first-in, first-out, non-queue basis.").

Moreover, J-STD-025 is not deficient for failure to set an explicit maximum delivery time. CALEA does not require any such provision to be included in an industry standard. Indeed, the arbitrariness of the three second maximum proposed in the DOJ/FBI Petition is illustrated by the fact that DOJ and FBI proposed a ten second maximum as recently as December 1997.[168] J-STD-025 already provides for immediate delivery (which will almost always occur within three seconds), with an appropriate exception for CDC congestion. These provisions are fully compliant with CALEA.

2. Synchronization of the Call Data Channel

The DOJ/FBI request for synchronization of CDC messages to within 100 milliseconds of triggering events is even further from the statute. The relevant provision of CALEA requires only that call-identifying information be provided "in a manner that allows it to be associated with the communication to which it pertains."[169] It does not require a script of all events during the call, let alone a script accurate to 100 milliseconds. J-STD-025 fully satisfies the statutory requirement by providing that each message on a CDC will include sufficient information to identify the communication to which the message relates. It even goes further, calling for a time stamp indicating the time at which the triggering event was detected by the network at the intercept access point ("IAP") – i.e., the point within the network used to access call-identifying information for the purpose of an

---

[168] FBI December 1997 Clarifications at 1. At other times, law enforcement has suggested even more burdensome timing requirements. See, e.g., February 1997 Punch List at 3 (500 millisecond maximum).

[169] 47 U.S.C. § 1002(a)(2)(B).